ADDITIONAL FEE:

Please charge any insufficiency of fee, or credit any excess, to Deposit Account No. 50-0427.

## R E M A R K S

The Office Action issued August 13, 2003 has been received and its contents have been carefully considered.

Applicant has amended claim 72 to render it more clear and definite, and has amended independent claim 88 to incorporate the subject matter of dependent claims 89 and 90, respectfully.

The present invention concerns a method and apparatus for generating original documents from a secure source, using a computer, which cannot be duplicated. Any forged or counterfeit copy of such an original document, that was produced in accordance with the invention, is detectable as a forgery.

Terminology:

Before explaining the invention in detail, it is useful to consider the particular terminology that has been used in the present application and that will be used in discussing

the invention. The following terms are not, precisely speaking, "synonyms" but are alternate words and phrases that have similar meanings. Sometimes the words or phrases that follow the terms have different or more specific meanings than the terms themselves, but they are included below because they are a component of the primary meaning.

Document stock := recording medium, blank document, media

Document content := subject matter printed on document stock

Unique document identifier := non-deterministic characteristic, serial number

Normalized document := normalized space, transformation of scanned document, transformation of document source

Distinct identification := digital digest, MD5, SHA-1

Unit of blank stock := sheet of paper

Imprinted := is used when the process could be printing on stock or imprinting on a plastic card or other suitable media

Present Invention:

To generate original documents that cannot be forged or counterfeited, the present invention provides a method and apparatus that combines the following three elements:

ELEMENT 1 - Counterfeit resistant blank stock. Each unit of the document stock contains its own unique identification.

In particular the blank stock can be paper. The paper may contain separate means for achieving counterfeit resistance and unique identification or these means may be combined together. A single feature such as microfilament distribution could provide both the counterfeit resistance and the unique identification. A second way to provide both unique identification and counterfeit resistance is to infuse uniquely tagged nanotubes into the paper, and to detect the nanotubes by an automatic reading device at the point of imprinting the contents. In these two prior art techniques, the unique identifier is determined just prior to imprinting the document.

Only a single counterfeit-resistant method or means needs to be used, but several -- such as micro-printing, ink

with differential color direction, invisible ink that shows up on copying, and embedded metallic fibers -- may be used in combination.

There are a large number of ways to give both unique identification and counterfeit resistance. Many of these are used in the printing of money. These two qualities can also be fairly easily added to other media such as a plastic card.

ELEMENT 2 - Imprinting information on the blank stock where the information has a distinct identification.

The media could be paper, and the information could be a text document or a graphic picture. The distinct identification of a text document is represented by a number often called a "digital digest". This distinct identification could be computed by a hash function such as MD5, SHA-1, or the sum of the ASCII representation of each character. For a graphic it could be something such as the total area occupied by each of three colors.

It is hard to imagine any kind of information that could be imprinted on blank stock that does not have a distinct identification that can be quantized.

Many distinct identification algorithms have been developed in order to protect against changes in the underlying information. The earliest ones used were called "check sums", which were used to confirm that a block of text had been successfully transmitted or successfully read from a disk. More elaborate algorithms are used in modern information exchange to ensure that a digital document has not been tampered with.

The common use of this distinct identification is to compute a number before the document is stored or transmitted and then either to convey this number separately to the recipient or to append it to the document. The recipient then independently computes the distinct identification and compares it with the number computed before the document was stored. If these two numbers agree, then it is assumed that no change has been made to the document. With the present invention this method of verification is extended to the imprinted document.

The document content for the secure documents, according to the invention, may be obtained from any electronic source, such as a database or over the Internet. In view of the sensitivity of the document content as well

as the documents themselves, this content is usually obtained from a source which is known to be secure.

ELEMENT 3 - The cryptographic combination of the unique identification of element 1 with the distinct identification of element 2, and its storage on the document stock.

In the preferred embodiment of the invention, the public/private key method is used to encrypt this information. The unique identification of element 1 and the distinct identification of element 2 are optionally combined with other information about the document and digitally encrypted with a private key. This encrypted message is imprinted on the bottom of the document.

The purpose of this cryptographic combination is to be able to authenticate that the document is unaltered. Authentication occurs when this string is signed with the public key to reveal the unique identification of element 1 and the distinct identification of element 2. Only the knowledge of the private key would allow someone else to produce the string unlocked by the public key.

An additional advantage of this cryptographic combination is that other information related to the

document, such as the identity of the sender, a unique document index, and the time and date the document was signed, can also be included in the data to be encrypted by the private key and, therefore, can be authenticated later by decrypting this stored string of characters with the public key.

Examples:

The present invention contemplates and makes possible the following three examples. In each of these examples validation can be performed without connection to the Internet or an internal table of valid receipts. Apparatus in the form of a standalone device must contain a scanner, a formula for computing the digital digest, a formula for decrypting a string of data, and the public key for the type of document being validated. The standalone device could be made sufficiently small that it could fit into a pocketbook or even a pocket.

Example 1

A stock certificate form is preprinted using a counterfeit-resistant method and is uniquely identified with

a serial number. At a later time the stock certificate details are printed on the form, and a digital digest of this printed information is cryptographically combined with the preprinted document number and printed on the bottom of this form.

Example 2

"A tamper proof voting trail that can be audited."

The present invention allows electronic balloting machines anywhere in the world to produce a secure paper record of each individual voter's vote: a record that absolutely cannot be altered without detection. Because the ballots cannot be copied without detection, they can provide comforting security to voters in countries around the world who ask the question, "How do we know the computer actually counted our vote?"

The individual voter receives from a polling administrator a blank paper ballot, which contains a preprinted serial number. The voter enters an electronic voting booth and inserts the paper ballot into the voting machine. He casts and confirms his vote electronically. The voting machine then prints a record of the individual's vote onto the blank paper ballot in an unalterable form and

returns this completed ballot receipt to the voter. The voter then exits the polling booth retaining this ballot receipt as a personal copy of his voting record.

The ballot receipt is similar in concept to the receipt taken by a person after an ATM transaction but with the added element of paper document security. The individual's voting record is cryptographically tied to the preprinted serial number on the ballot receipt. Although the voting machine maintains a complete electronic record, the machine could fail, or unscrupulous hackers might access and alter the record. Nothing, however, can alter the ballot receipt retained by the voter.

Preprinted blank paper ballots are protected by the same counterfeit resistance and unique identification that is characteristic of paper currency. This document stock could be printed by the same companies that currently print paper currency.

The inherent security of the ballot receipts produced in accordance with the present invention is such that they could also be used for an election recount. A ballot receipt does not directly reveal the identity of the individual voter but could be used at any time for proof of

how a group of people voted. Anonymity of the individual would be protected while still giving an exact summary of the votes of a pool of voters.

If someone challenged the results of an election, the ballot receipts could be used for a recount even if the voting computers were totally destroyed. In such an event (an election recall) individual voters could return to the voting polls and have their ballot receipts electronically re-tabulated. Because of cryptographic digital signatures, there would be no possibility that these ballots could have been produced in any way other than by voting in the specified election under challenge.

The present invention which generates the ballot receipts is totally immune from fraud and can be used in a variety of applications and elections.

Other variations are possible. For example:

- A plastic card could be used to hold the magnetic imprinting of the voting record.
- The voting record could be scrambled so that the only way to reveal it would be by use of a password. The problem of relying on passwords is that people might forget them.

The voting machine might imprint two ballot receipts, one of which the voter would have to deposit into a sealed box as he or she exits the polling booth. This variation would make it easier to spot check electronic tallies with the tallies based solely on the ballot receipts deposited into the sealed box. A further check could be done by asking voters to return to the polling place with their ballot receipts.

Example 3

A driver's license or other government-issued certificate could have a summary line on the bottom of the certificate with a specialized line of printed characters just below that. This would make it possible for a palm-sized scanner to validate the certificate in the absence of a connection to a database or to an on-line service. This would also facilitate remote printing in kiosks of important government documents and thus further facilitate the use of electronically generated Government documents.

Prior Art Rejection:

Claims 53-57 and 72-93 stand rejected as being unpatentable over the U.S. Patent No. 5,991,399 to Graunke et al. in view of the U.S. Patent No. 5,873,604 to Phillips. This rejection is respectfully traversed for the reasons given below.

U.S. Patent No. 5,991,399

The Graunke patent describes a clever way to transmit encryption keys to a remote site, called a "trusted player" in the patent, where items may be decrypted, and presumably played, using public/private key encryption. There is mention of payment for the use of the key.

The present invention may use public/private key encryption; however, the applicant does not claim any patent protection for this particular encryption method or for transmission of keys. The encryption used in the third element of the invention, discussed above, can be any kind of encryption, not simply public/private key encryption.

U.S. Patent No. 5,873,604

The abstract of this patent describes a process that claims to validate that a paper document is the one that was actually printed.

> "The use of both thermochromic pantograph and validation mark in the present invention provides multiple levels of protection against the unauthorized alteration or counterfeiting of valuable documents."

This patent discloses and claims a very sophisticated way of producing BLANK stock for documents to be later printed. The present invention is not concerned with any such method for producing document stock but, rather, uses document stock that is counterfeit resistant as one of the requirements of the first element. The present invention requires that each unit of the document stock contains its own unique document identifier. There is no mention in the Phillips patent of such a unique identification.

The Phillips patent does not claim to detect multiple printings, whereas the present invention can detect any unauthorized imprinting on document stock. The Phillips patent does not claim to detect changes in the document made from a screen capture program prior to printing, whereas the

present invention can detect any such change. Most importantly, if a forger were to obtain Phillips' "document stock" and then print forgeries on this stock, there would be no way of detecting such forgeries, whereas with the present invention any unauthorized imprinting on the document stock is easily detected.

With the present invention even a person having intimate access to the document stock, to the imprinting, and to the program used to imprint, could not produce an altered document without it being detected as a fraud. Furthermore, the invention meets the qualifications of a digital signature for each page, and therefore these documents are covered by all the laws having to do with digital signatures.

Furthermore, the Phillips patent claim 1 sets forth the requirement of "a first surface and a second surface." However, the present invention does not require a first and second surface and can utilize ordinary paper stock.

In summary, the present invention ties together the precise contents of the document with a specific unit of document stock. Consequently, if someone were to obtain copies of this original document stock, any unauthorized

documents that were produced from this stock could be detected as forgeries.

Applicant's independent claims 53, 72 and 88 all recite the combination of the three elements which make this forgery detection possible. Claim 53 recites:

> "authenticating the counterfeit resistant document by authenticating the security feature and comparing the stored document content with a perceived document content."

Claim 72 now recites:

> "generating an associated digital signature for verification of the document content and said essentially unique identifier; and
>
> printing the content and the digital signature on the document stock by means of a computer printer."

Finally, claim 88 recites:

> "information content recorded on the content recording surface; and
>
> a self-authenticating message recorded on the content recording surface for authenticating the information content and the tamper resistant unique identifier."

In conclusion, therefore, applicant's independent claims 53, 72 and 88 recite methods of authenticating a document, and an authenticatable recording medium, respectively, which distinguish patentably over the cited references.

This application is therefore believed to be in condition for immediate allowance. A formal Notice of Allowance is accordingly respectfully solicited.

Respectfully submitted,

By _____
Karl F. Milde, Jr.
Reg. No. 24,822

MILDE & HOFFBERG, LLP
10 Bank Street - Suite 460
White Plains, NY 10606
(914) 949-3100

I hereby certify that this correspondence is being deposited with the United States Postal Services as first class mail in an envelope addressed to: Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450 on

JULY 13, 2004

MILDE & HOFFBERG, LLP

By _____

Date JULY 13, 2004